Using Group Policy Object Templates with RSA Authentication Agent 7.0 for Microsoft Windows

Revision 1

The Security Division of EMC

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **www.rsa.com**

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the **thirdpartylicenses.html** file.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

First printing: March 2008
Revised: December 2010

Revision History

Revision Number	Date	Revision
1	December 2010	• Added Password Synchronization template

Contents

Preface

About This Guide

This guide describes how administrators can use Group Policy Object templates to manage RSA Authentication Agent 7.0 for Microsoft Windows (Authentication Agent). When combined with RSA Authentication Manager 6.1 with Patch 2 or later, or with RSA Authentication Manager 7.1, Authentication Agent enhances native Windows security with strong, two-factor authentication using RSA SecurID tokens.

RSA Authentication Agent 7.0 for Microsoft Windows Documentation

For more information about RSA Authentication Agent 7.0 for Microsoft Windows, see the following documentation and Help:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest *Release Notes* version is available from RSA SecurCare Online: **https://knowledge.rsasecurity.com**.

RSA Authentication Agent 7.0 for Microsoft Windows Installation and Administration Guide. Provides instructions on how to install, configure, troubleshoot, repair, or remove the product.

RSA Security Center Help. Describes the user options available in the RSA Security Center (the user interface of RSA Authentication Agent). All of the user options appear in the **Home** tab. To view the Help, click **Help** from the RSA Security Center menu or any dialog box.

RSA Security Center Administrator Help. Describes the configuration options available to administrators in the RSA Security Center (the user interface of RSA Authentication Agent). All of the administrator options appear in the **Configuration** tab. Any changes made through the Security Center only affect the local computer. To view the Help, click **Help** from the RSA Security Center menu or any dialog box.

Related Documentation

For more information about the products related to RSA Authentication Agent 7.0 for Microsoft Windows, see the following:

RSA Authentication Manager documentation set. The full documentation set for RSA Authentication Manager 6.x or 7.x. To access a documentation set, go to **http://knowledge.rsasecurity.com**.

RSA Secured Partner Solutions directory. RSA has worked with a number of manufacturers to qualify software that works with RSA products. Qualified third-party products include virtual private network (VPN) and remote access servers (RAS), routers, web servers, and many more. To access the directory, including implementation guides and other information, go to **http://www.rsasecured.com**.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes Implementation Guides with step-by-step instructions and other information about using RSA products with these third-party products.

Before You Call Customer Support

Make sure that you have direct access to the computer running the RSA Authentication Agent 7.0 for Microsoft Windows software.

Please have the following information available when you call:

- ❑ Your RSA Customer/License ID for Authentication Manager.
- ❑ RSA Authentication Agent for Microsoft Windows software version number.
- ❑ The make and model of the machine.
- ❑ The name and version of the operating system.

1 Understanding the Group Policy Object Templates

This chapter describes the options you can set in the Group Policy Object (GPO) templates to manage RSA Authentication Agent for Microsoft Windows. For details on installing the templates on the domain controller and setting the options, see Chapter 2, "Configuring Group Policy Object Template Settings."

Overview of Authentication Agent for Microsoft Windows

RSA Authentication Agent 7.0 for Microsoft Windows works with RSA Authentication Manager 6.1 with Patch 2 or later, or with RSA Authentication Manager 7.1, to protect your company's resources. Authentication Agent uses two-factor authentication to protect access to computers with a Windows Vista or later operating system. Two-factor authentication requires something you know (for example, an RSA SecurID PIN) and something you have (for example, a tokencode generated by an RSA SecurID token).

Note: You must use a hand-held RSA SecurID token with RSA Authentication Agent. For example, you cannot use a software token on your computer or a SecurID token connected to the USB port. But, you can use Authentication Agent with a software token installed on a portable device, for example, a Blackberry. For more information on software tokens, see the RSA documentation that came with your software token.

If you require a user to log on through Authentication Agent, the user may need to enter an RSA SecurID PIN followed by a tokencode to access the computer. The SecurID PIN and tokencode are known as the passcode. The first time users authenticate with passcodes, they create their SecurID PINs (automatically or manually). The tokencode appears as numbers on the front of a handheld SecurID token. The numbers change approximately every minute.

When a user enters a passcode, Authentication Agent sends the passcode to Authentication Manager for validation. If the passcode is correct, the user gains access to the desktop. Authentication Agent intercepts attempts to access local Windows desktops on users' workstations and prompts users for RSA SecurID passcodes.

To deploy local authentication, you can use the configuration wizard to configure options and deploy it to multiple desktops. Once installed, you can manage Authentication Agent on individual computers through the RSA Security Center (user interface of Authentication Agent) or use the Group Policy Object templates to manage multiple computers. For more information on using the configuration wizard, see the *RSA Authentication Agent 7.0 for Microsoft Windows Installation and Administration Guide*. For more information on managing options for a local computer, see the RSA Security Center Administrator Help.

Overview of the Group Policy Object Templates

RSA Group Policy Object templates make it easier for you to manage Authentication Agent on many computers after you deploy it. To use the Group Policy Object templates, you load them into the Microsoft Policy Management tool on your domain controller and specify authentication policy settings in the templates. Each workstation within the domain automatically downloads the settings and then loads them into the Microsoft Registry.

In domain environments, all computers wait for specified refresh intervals before updating their settings. Once the refresh process ends, settings associated with the templates load into the Microsoft Registry. The settings specified in the Group Policy Object templates override the settings configured on individual workstations.

Important: The RSA templates are not policies. Windows stores RSA settings under **HKEY_LOCAL_MACHINE** > **Software** > **RSA** in the Registry Editor keys because they are preference settings instead of policy settings. For more information, see "Local Authentication Template" on page 12 or "Password Synchronization Template" on page 15.

The Authentication Agent supports the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**). It allows you to define policy settings to control how Authentication Agent requires users to authenticate. The Authentication Agent also supports the Password Synchronization template (**RSA_AuthAgent_PassSynch.adm**). This allows you to define policy settings to control the synchronization of domain user password changes with the passwords in the Authentication Manager database.

These templates do not automatically come with the product. To obtain these Group Policy Object templates, go to the Authentication Agent product page on the RSA web site (**www.rsa.com**) and see the download page. (Go to the RSA Authentication Agent **Try/Evaluate page** and click **Downloads** from the bottom of the page.)

Supporting GPO Templates in a 6.x and 7.x Mixed Environment

If a domain environment consists of both 6.x and 7.x Authentication Agents on individual client machines, you must install two sets of GPO templates on the domain controller or controllers in your environment. One set is for the Local Authentication template, which must be installed on domain controller(s) for the client machines. The other set is for the Password Synchronization template, which must be installed on every domain controller in your environment.

Local Authentication Template

The Local Authentication template allows you to define policy settings to control how Authentication Agent requires users to authenticate. This template pushes out Local Authentication Client (LAC) settings to the client machines. If you have both 6.x and 7.x Authentication Agents on individual client machines in your environment, you must install both the 7.x Local Authentication template (**RSA_AuthAgent_LocalAuth.adm)** and the 6.x Local Authentication template (**RSA_SID_Agent.adm**) on the domain controller(s) for these machines.

Password Synchronization Template

The Password Synchronization template allows you to define policy settings to control the synchronization of domain user password changes with the passwords in the Authentication Manager database. To support Password Synchronization for domain users, the RSA Authentication Agent must be installed on every domain controller in the local network along with the corresponding version of the Password Synchronization template.

Note: The characteristic Agent installation on a domain controller is a non-enabled Local Authentication Client (LAC). The sole purpose of the installation of the Agent is to install the Password Synchronization component of the Agent, which is then triggered on domain user password changes. This trigger reports the domain user password change back to the Authentication Manager. The Password Synchronization template applies only to domain controllers.

The version of Authentication Agent to install on a Windows 2008 Server is RSA Authentication Agent 7.x for Microsoft Windows.The version of Authentication Agent to install on a Windows 2003 Server is RSA Authentication Agent 6.x for Microsoft Windows.

The Password Synchronization template to install with a version 7.x Authentication Agent is (**RSA_AuthAgent_PassSynch.adm**). Installing and choosing the settings for the Password Synchronization template (**RSA_AuthAgent_PassSynch.adm**) is covered in Chapter 2, "Configuring Group Policy Object Template Settings."

The Password Synchronization template to install with a version 6.x Authentication Agent is (**RSA_SID_PFC.adm**). For information on installing and choosing the settings for the Password Synchronization template (**RSA_SID_PFC.adm**), see the *Using Group Policy Object Templates to Manage RSA Authentication Agent* guide for version 6.1 or 6.4 on the RSA Authentication Agent **download page**. Either of the Password Synchronization templates (for 6.x or 7.x) can be found from the Authentication Agent download page. (Go to the RSA Authentication Agent **Try/Evaluate page** and click **Downloads** from the bottom of the page.).

Local Authentication Template

The Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) contains preference settings that you define to control how Authentication Agent appears to users. For example, you can specify what Credential Provider (logon prompt options) you want users to see, define challenge groups, set the logon field label, send the domain and user name to Authentication Manager, and define the ability to unlock the computer with an RSA SecurID PIN instead of a full passcode (PIN and tokencode). (You can also find these settings under the **Configuration** tab of the RSA Security Center.)

The Local Authentication template has the following two preference settings folders:

- Credential Provider Settings
- Local Authentication Settings

Important: The RSA templates are not policies. They are preference settings. Policies include settings that Windows stores in the Registry Editor keys under **Software** > **Policies**. Windows stores the RSA preference settings under **HKEY_LOCAL_MACHINE** > **Software** > **RSA** in the Registry Editor keys. You do not find them under **Policies**. If you configure a policy setting, the changes take effect as soon as they deploy to the computers in the domain. If you configure a preference setting, it also takes effect as soon it deploys through the domain. But, if you later decide to clear a preference setting and place it in an "unconfigured" state, Windows cannot apply the change (as it can with a policy setting). Instead, it retains the last setting you used. For example, if you enabled the Credential Provider filter setting and selected the **Show all available Credential Providers** options, users can see all the available logon tiles to log on to the computer. If you later access the preference again and select the **Not Configured** option, Windows retains the **Show all available Credential Providers** setting. Users will continue to see all the available logon tiles. You must select another option for the setting or select **Disable** to clear it.

Each preference folder contains subfolders. The subfolders contain preferences with settings that allow you to control different authentication components. For details on the Credential Provider Settings and Local Authentication Settings preferences, see "Credential Provider Settings" on page 13 or "Local Authentication Settings" on page 14.

Credential Provider Settings

As described in the previous section, the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) contains the **Credential Provider Settings** and **Local Authentication Settings** preference folders. This section describes the Credential Provider Settings options. For details on the Local Authentication Settings options, see "Local Authentication Settings" on page 14.

The **Credential Provider Settings** folder contains a folder with the **Credential Provider Filter Type** setting. You can select one of the following for the setting:

- **Enable** (to activate)
- **Not Configured** (to leave inactive)
- **Disable** (to clear a previously enabled setting).

If you select **Enable**, you can select one of the following filtering types from the drop-down list:

- **Hide Microsoft Password Provider (default)**. Prevents users from logging on with Microsoft Windows passwords using the Microsoft Password Credential Provider. (Other Credential Providers remain available.) This is the default credential provider filter setting.
- **Only show RSA Authentication Agent Provider**. Prevents users from logging on using any method other than RSA SecurID passcodes.
- **Hide RSA Authentication Agent Provider**. Prevents users from logging on with RSA SecurID passcodes (PINs and tokencodes). (Other Credential Providers remain available.)
- **Show all available Credential Providers**. Allows users to log on using all available Credential Providers. Selecting this option ensures that users can log on to their workstations in case RSA SecurID is not available. For example, you may want to select this option until RSA SecurID is fully deployed throughout your company.

For more information on configuring the Credential Provider Filter Type preference, see "Defining the Credential Provider Settings" on page 23.

Local Authentication Settings

As described in "Overview of the Group Policy Object Templates" on page 10, the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm**) contains the **Credential Provider Settings** and **Local Authentication Settings** preference folders. This section describes the Local Authentication Settings options. For details on the Credential Provider Settings options, see "Credential Provider Settings" on page 13.

The **Local Authentication Settings** folder contains the **Challenge**, **Authentication**, and **Unlocking Computer** folders.

These folders contain different preferences that you can set. For example, you can allow or deny the ability for a local administrator to define challenge groups. You can also define the users and groups that you want Authentication Agent to challenge for a SecurID passcode (PIN and tokencode). And, you can determine if you want to allow users to unlock their computer with a SecurID PIN instead of a full passcode.

The **Challenge** folder contains these preference settings:

- **Deny Access to Local Authentication Challenge Settings for Local Administrators**
- **Challenge Users**
- **Specify Challenge Group**
- **Allow Retrieval of Locally Cached Challenge Settings**

You can define the settings to allow or deny the ability for a local administrator to define challenge groups. You can also define users and groups you want Authentication Agent to challenge for a SecurID passcode (PIN and tokencode) and allow Authentication Agent to locate the local cached challenge setting from a local cache if it cannot determine the challenge status due to a network connection failure. For example, you can select one of the following for the **Deny Access to Local Authentication Challenge Settings for Local Administrators** setting:

- **Enable** (to activate)
- **Not Configured** (to leave inactive)
- **Disable** (to clear a previously enabled setting).

The **Authentication** folder contains these preference settings:

- **Label for the Local Authentication Prompt**
- **Send Domain and User Name to Authentication Manager**

With these preferences, you can set the logon label (**Password** or **Passcode**) and allow Authentication Agent to send the domain and user name to Authentication Manager to keep the accounts synchronized for online and offline authentication.

The **Unlocking Computer** folder has these preference settings:

- **Unlock with RSA SecurID PIN**
- **RSA SecurID PIN Time-Out**
- **RSA SecurID PIN Attempts**

With these preferences, you can set the option to allow the user to unlock the computer with a PIN instead of a full passcode, define the time allowed to enter a PIN before Authentication Agent requires a passcode, and specify the number of PIN attempts you want to allow.

For more information on configuring the Challenge, Authentication, and Unlocking computer preferences, see ."Defining the Local Authentication Settings" on page 24.

Password Synchronization Template

The Password Synchronization template (**RSA_AuthAgent_PassSynch.adm**) enables you to specify categories of users for whom password changes made to their domain accounts are synchronized with their corresponding passwords in the Authentication Manager database. For password synchronization to work, you must install the Authentication Agent on every domain controller in your environment. The password synchronization component is installed when you install the Authentication Agent's default Agent type, "Local authentication component". Although you have to install the Authentication Agent on the domain controllers, you are not required to enable the RSA SecurID challenge on the domain controllers. The challenge and password synchronization are independent.

After installing the Authentication Agent, you must perform a test authentication using RSA SecurID. This establishes a node secret on the domain controller. The node secret is required for communication with RSA Authentication Manager. For installation information, see the chapter about installing the Authentication Agent in the *Installation and Administration Guide* for your platform.

The templates are the only way to configure domain password synchronization.

Important: The RSA templates are not policies. They are preference settings. Policies include settings that Windows stores in the Registry Editor keys under **Software** > **Policies**. Windows stores the RSA preference settings under **HKEY_LOCAL_MACHINE** > **Software** > **RSA** in the Registry Editor keys. You do not find them under **Policies**. If you configure a policy setting, the changes take effect as soon as they deploy to the computers in the domain. If you configure a preference setting, it also takes effect as soon it deploys through the domain. But, if you later decide to clear a preference setting and place it in an "unconfigured" state, Windows cannot apply the change (as it can with a policy setting). Instead, it retains the last setting you used. For example, assume you enable the **User Group** filter setting to specify which domain users' password changes are to be synchronized with the passwords in the Authentication Manager database and specified "Include" as the group name. If you subsequently want to remove the "Include" Group filter, you should do so by choosing the **Select Disabled** option rather than the **Not Configured** option.

Policy preferences for Password Synchronization are placed under one sub-folder, **Password Synchronization Settings**, under the folder **RSA Authentication Agent 7.0 for Microsoft Windows**. These preferences are:

- **Sychronize Users**

- **Specify User Group**
- **Send Domain and User Name to Authentication Manager**

Each of these preferences are controlled by modes:

- **Not Configured** (to leave inactive)
- **Enabled** (to activate)
- **Disabled** (to clear a previously enabled setting)

For more information on configuring Password Synchronization, see "Defining the Password Synchronization Preference Settings" on page 29.

2 Configuring Group Policy Object Template Settings

This chapter describes how to install and define the RSA Authentication Agent 7.0 for Microsoft Windows Group Policy Object settings.

Preparing to Install the RSA Group Policy Object Templates

Group Policy is a feature of Microsoft Windows. RSA recommends that before you deploy the RSA Group Policy Object templates, you become familiar with Microsoft Windows Group Policy concepts and best practices. For more information on Group Policy, go to the Windows Server Group Policy page in the Microsoft Support Knowledge Base at **http://www.microsoft.com/grouppolicy/**.

Important: The RSA templates are not policies. Policies include settings that Windows stores in the Registry Editor keys under **Software** > **Policies**. Windows stores RSA settings under **HKEY_LOCAL_MACHINE** > **Software** > **RSA** in the Registry Editor keys because they are preference settings instead of policy settings. This difference affects how Windows applies a setting if you define it and later want to set it to an "unconfigured" state. For more information, see "Local Authentication Template" on page 12 or see "Password Synchronization Template" on page 15.

As an alternative to using the RSA Group Policy Object templates, you can apply preference settings by incorporating them in logon scripts. For more information, see "Configuring Preference Settings Using Logon Scripts" on page 38.

Installing GPO Templates in a 6.x and 7.x Mixed Environment

If a domain environment consists of both 6.x and 7.x Authentication Agents on individual client machines, you must install two sets of GPO templates on the domain controller or controllers in your environment. One set is for the Local Authentication template, which must be installed on domain controller(s) for the client machines. The other set is for the Password Synchronization template, which must be installed on every domain controller in your environment.

Local Authentication Template

The Local Authentication template allows you to define policy settings to control how Authentication Agent requires users to authenticate. This template pushes out Local Authentication Client (LAC) settings to the client machines. If you have both 6.x and 7.x Authentication Agents on individual client machines in your environment, you must install both the 7.x Local Authentication template (**RSA_AuthAgent_LocalAuth.adm)** and the 6.x Local Authentication template (**RSA_SID_Agent.adm**) on the domain controller(s) for these machines.

Password Synchronization Template

The Password Synchronization template allows you to define policy settings to control the synchronization of domain user password changes with the passwords in the Authentication Manager database. To support Password Synchronization for domain users, the RSA Authentication Agent must be installed on every domain controller in the local network along with the corresponding version of the Password Synchronization template.

Note: The characteristic Agent installation on a domain controller is a non-enabled Local Authentication Client (LAC). The sole purpose of the installation of the Agent is to install the Password Synchronization component of the Agent, which is then triggered on domain user password changes. This trigger reports the domain user password change back to the Authentication Manager. The Password Synchronization template applies only to domain controllers.

The version of Authentication Agent to install on a Windows 2008 Server is RSA Authentication Agent 7.x for Microsoft Windows.The version of Authentication Agent to install on a Windows 2003 Server is RSA Authentication Agent 6.x for Microsoft Windows.

The Password Synchronization template to install with a version 7.x Authentication Agent is (**RSA_AuthAgent_PassSynch.adm**). Installing and choosing the settings for the Password Synchronization template (**RSA_AuthAgent_PassSynch.adm**) is covered in this chapter.

The Password Synchronization template to install with a version 6.x Authentication Agent is (**RSA_SID_PFC.adm**). For information on installing and choosing the settings for the Password Synchronization template (**RSA_SID_PFC.adm**), see the *Using Group Policy Object Templates to Manage RSA Authentication Agent* guide for version 6.1 or 6.4 on the RSA Authentication Agent **download page**. Either of the Password Synchronization templates (for 6.x or 7.x) can be found from the Authentication Agent download page. (Go to the RSA Authentication Agent **Try/Evaluate page** and click **Downloads** from the bottom of the page.).

Installing the RSA Group Policy Object Templates

The procedure for installing the templates varies, depending on the tool you use to launch the Group Policy Editor. The following procedures describe how to install the templates using the Active Directory Users and Computers Microsoft Management Console.

To install the templates on the domain controllers in the network:

1. Do one of the following:
   a. To install the Local Authentication template, copy the file **(RSA_AuthAgent_LocalAuth.adm)** to a local drive on one domain controller.

b. To install the Password Synchronization template, copy the file (**RSA_AuthAgent_PassSynch.adm**) to a local drive on all domain controllers.

2. Click **Start > Administrative Tools > Active Directory Users and Computers**.
3. From the Active Directory Users and Computers console, do one of the following:
   a. If you are installing the Local Authentication template, right-click the name of the domain where you want to install the Local Authentication template, and click **Properties**.
   b. If you are installing the Password Synchronization template, right-click **Domain Controllers** under the name of the domain where you want to install the template, and click **Properties**.
4. In the Properties dialog box, click the **Group Policy** tab. Select the policy where you want to add the template, and click **Edit**.
5. Click **Computer Configuration**. Then right-click **Administrative Template** and click **Add/Remove Templates** to open the Add/Remove Templates dialog box.
6. Click **Add**.
7. Do one of the following:
   a. To install the Local Authentication template, browse to the location of the (**RSA_AuthAgent_LocalAuth.adm**) file and click **Open**.
   b. To install the Password Synchronization template, browse to the location of the (**RSA_AuthAgent_PassSynch.adm**) file and click **Open**.
8. Click **Close**. You have installed the Local Authentication and/or the Password Synchronization templates. Once you install a template on a domain controller, it applies the settings to all the computers on the domain. The preference settings default to a **Not Configured** state. To enable any of the settings, see the following sections.

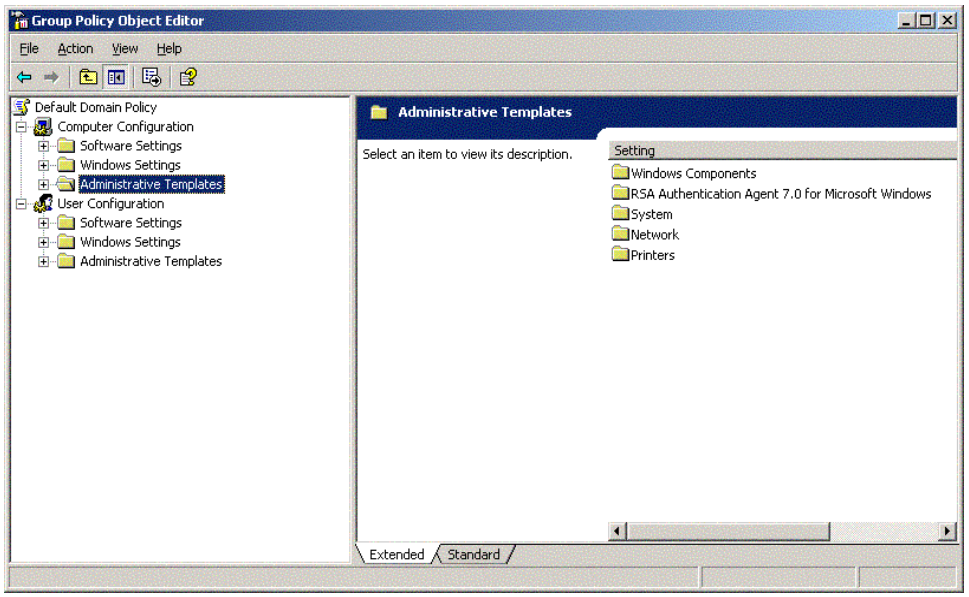
Note: In domain environments, all computers wait for specified refresh intervals before updating their settings. Once the refresh process ends, settings associated with the templates load into the Microsoft Registry. The settings specified in the Group Policy Object templates override the settings configured on individual workstations.

Defining the Local Authentication Preference Settings

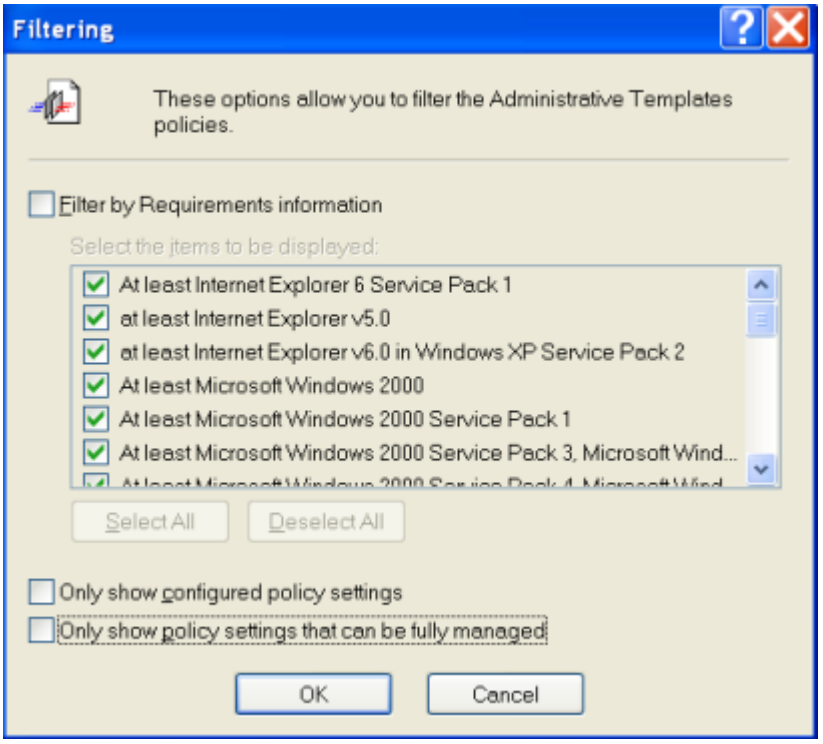
This section describes how to define the preference settings in the Local Authentication template (**RSA_AuthAgent_LocalAuth.adm).**

To define the settings in the Local Authentication template:

1. On the domain controller, click **Start > Administrator Tools > Active Directory Users and Computers**.
2. In the Active Directory Users and Computers dialog box, right-click the name of the domain, and click **Properties**.
3. Click the **Group Policy** tab.
4. In the Group Policy dialog box, click **Default Domain Policy**, then click **Edit**.
5. In the left pane of the Group Policy window, click **Administrative Templates** .Right-click **Administrative Templates > View > Filtering**.

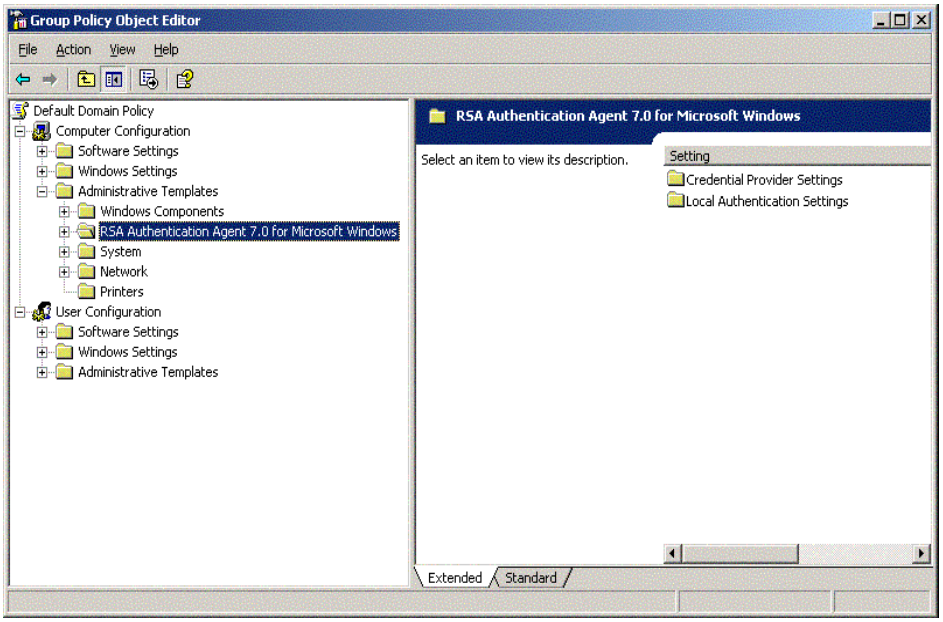


6. In the Filtering dialog box, clear **Only show policy settings that can be fully managed**. Because the RSA group policies are preferences and not true policies, you must clear this option to view the RSA Group Policy Object templates.



7. Click **OK**.

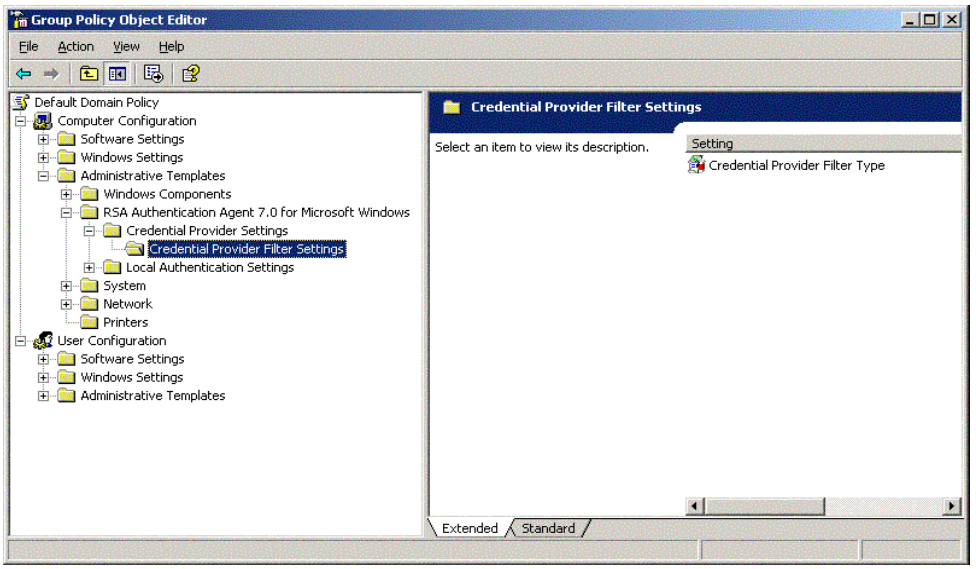
8. Double-click **Computer Configuration > Administrative Templates > RSA Authentication Agent 7.0 for Microsoft Windows**. You see the **Credential Provider Settings** and **Local Authentication Settings** preference folders as shown:



9. Click on the folders to access the preferences. For details on defining the Credential Provider Settings, see "Defining the Credential Provider Settings" on page 23. For details on defining the Local Authentication settings, see "Defining the Local Authentication Settings" on page 24.

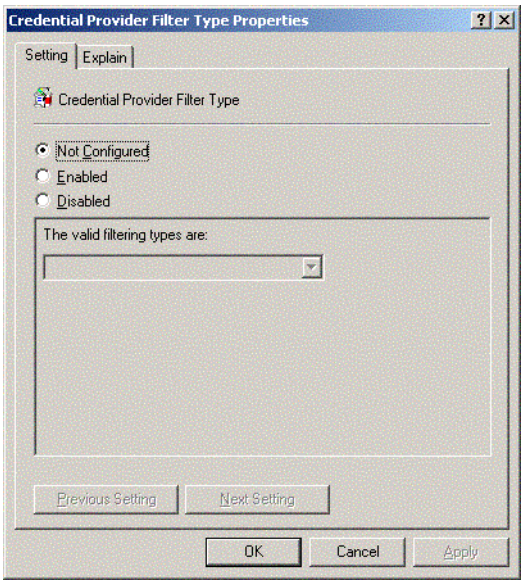
Defining the Credential Provider Settings

The **Credential Provider Filter Settings** folder contains the **Credential Provider Filter Type** preference as shown:



To define the Credential Provider Filter Type setting:

1. Double-click **Credential Provider Filter Type** to open the Credential Provider Filter Type Properties dialog box. For example:

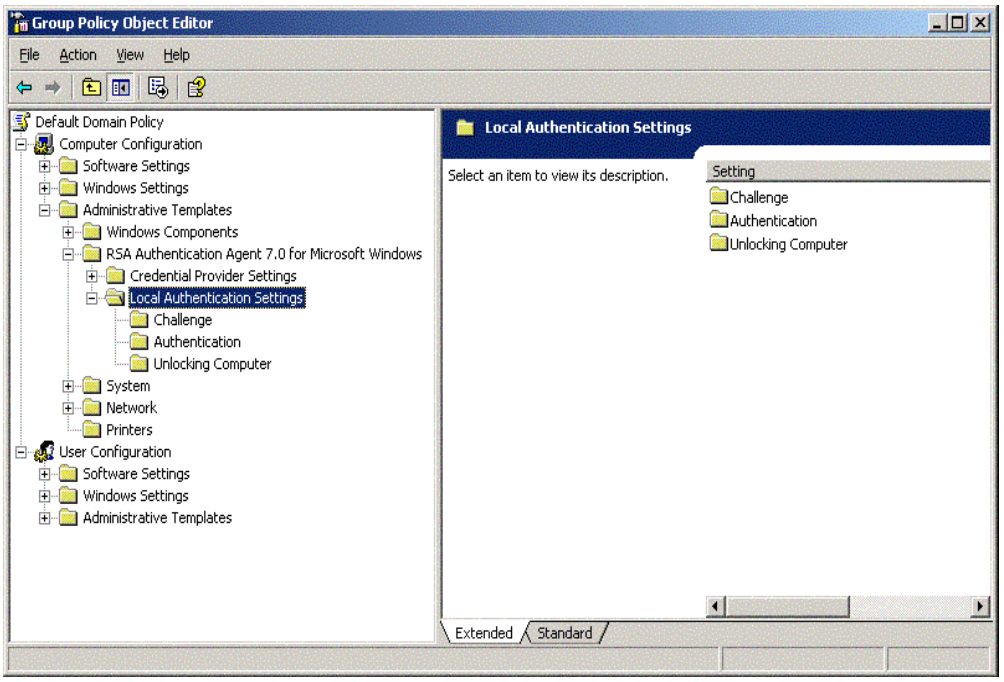


Note: Click the **Explain** tab to review a definition of the preference setting.

2. In the **Setting** tab, do one of the following:
   - Leave the default of **Not Configured** to leave the setting inactive.
   - Select **Enable** to activate the field setting. Then select one of the following from the drop-down list:
     - **Hide Microsoft Password Provider (default)**. Prevents users from logging on with Microsoft Windows passwords using the Microsoft Password Credential Provider. (Other Credential Providers remain available.) This is the default credential provider filter setting.
     - **Only show RSA Authentication Agent Provider**. Prevents users from logging on using any method other than RSA SecurID passcodes.
     - **Hide RSA Authentication Agent Provider**. Prevents users from logging on with RSA SecurID passcodes (PINs and tokencodes). (Other Credential Providers remain available.)
     - **Show all available Credential Providers**. Allows users to log on using all available Credential Providers. Selecting this option ensures that users can log on to their workstations in case RSA SecurID is not available. For example, you may want to select this option until RSA SecurID is fully deployed throughout your company.
   - Select **Disable** to clear the setting.
3. Click **Apply** to apply your changes. Then click **OK** to return to the **Credential Provider Filter Type** preference.

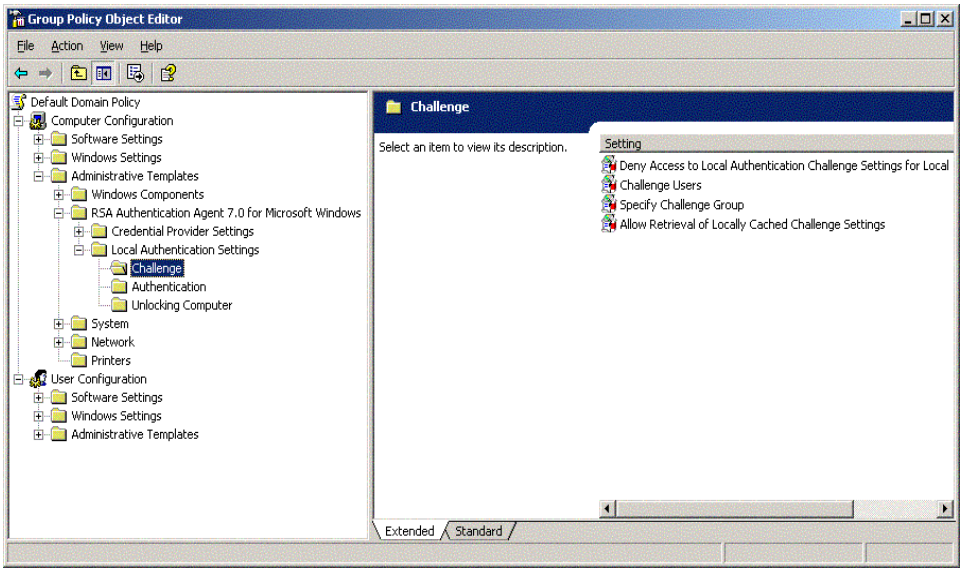
Defining the Local Authentication Settings

The **Local Authentication Settings** folder contains the **Challenge**, **Authentication**, and **Unlocking Computer** subfolders as shown:

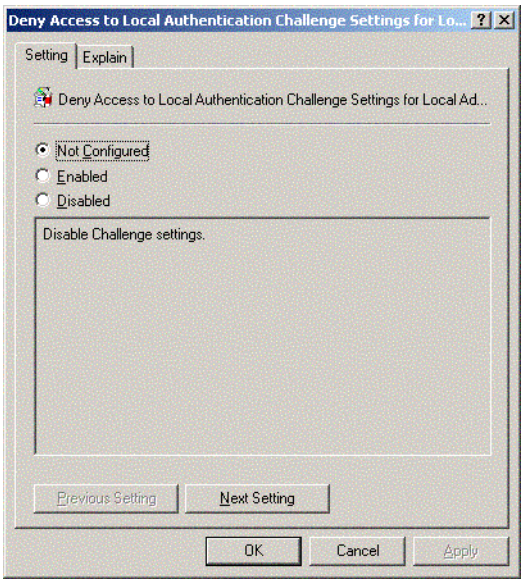


To define the Challenge setting:

1. Double-click the **Challenge** folder. You see the **Deny Access to Local Authentication Challenge Settings for Local Administrators**, **Challenge Users**, **Specify Challenge Group**, and **Allow Retrieval of Locally Cached Challenge Settings** preferences as shown:



2. Click the preference you want to set. For example, if you want to set the **Deny Access to Local Authentication Challenge Settings for Local Administrators** preference, click it to open the Deny Access to Local Authentication Challenge Settings for Local Administrators Properties dialog box:

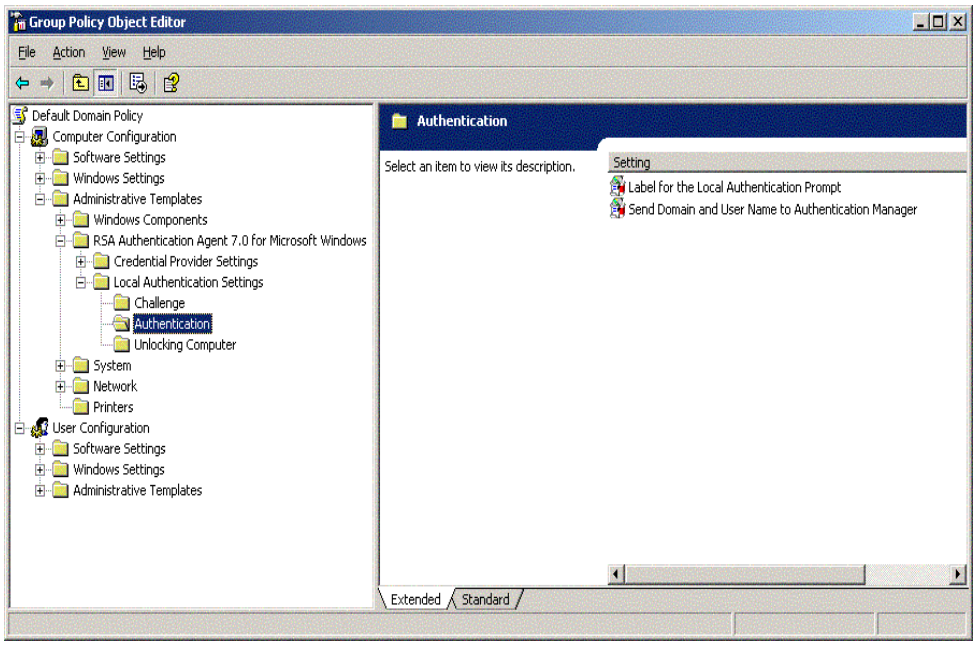


Note: Click the **Explain** tab to review a definition of the preference setting.

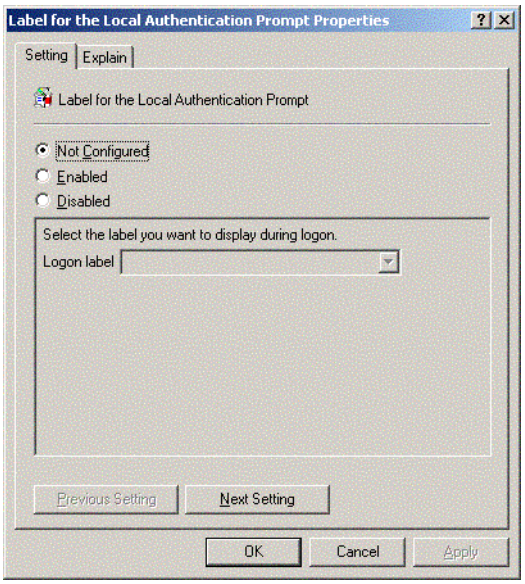
3. In the **Setting** tab, do one of the following:
   - Leave the default of **Not Configured** to leave the setting inactive.
   - Select **Enabled** to activate the field setting. This allows local administrators to define challenge users and groups.
   - Select **Disabled** to clear the setting.
4. Click **Apply** to apply your changes. Then click **OK** to return to the **Challenge** preferences.
5. Repeat the steps in this procedure for each preference you want to set. For example, if you to enable the **Challenge Users** preference**,** select **Off, Users In, All users**, or **All users except** from the drop-down list. Then enable the **Specific Challenge Group** preference and enter the name of the group you want to challenge in the **Group name** field. If you want to all allow Authentication Agent to locate the user's challenge setting from a local cache if it cannot determine the challenge status due to a network connection failure, enable the **Allow Retrieval of Locally Cached Challenge Settings** preference.

To define the Authentication setting:

1. Double-click the **Authentication** folder. You see you see the **Label for the Local Authentication Prompt** and the **Send Domain and User Name to Authentication Manager** preferences as shown:



2. Click the preference you want to set. For example, if you want to set the **Label for the Local Authentication Prompt** preference, click it to open the Label for the Local Authentication Prompt Properties dialog box:

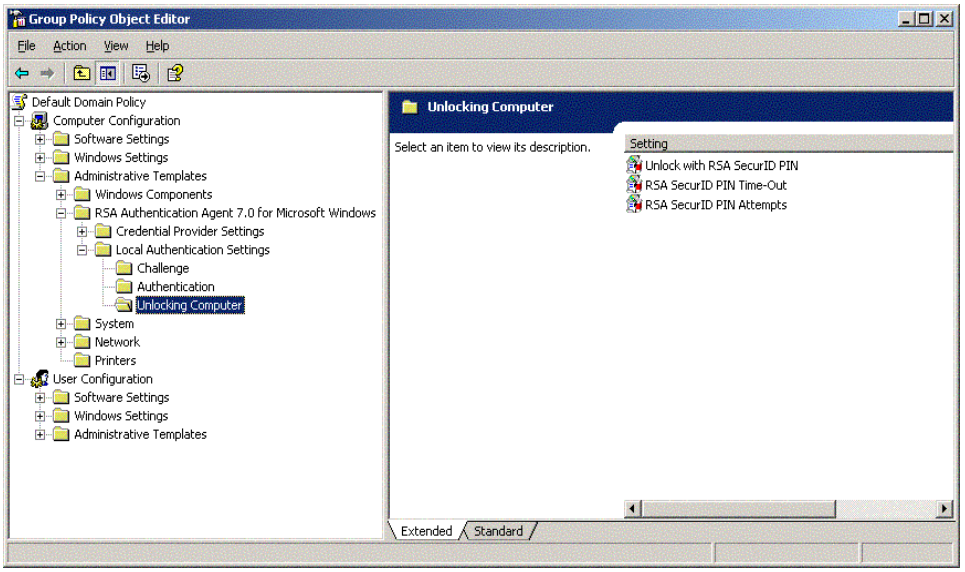


Note: Click the **Explain** tab to review a definition of the preference setting.

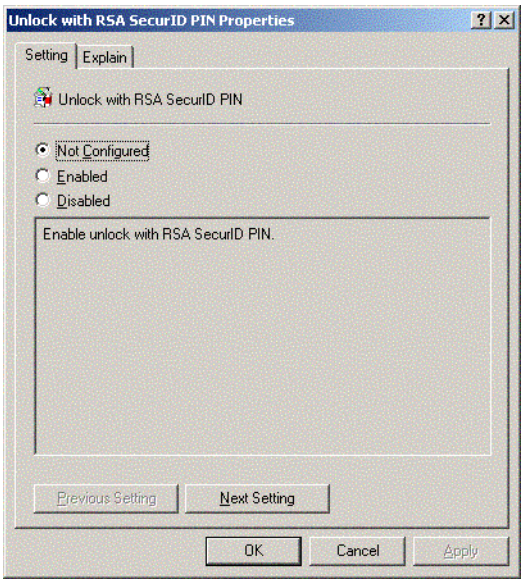
3. In the **Setting** tab, do one of the following:
   - Leave the default of **Not Configured** to leave the setting inactive.
   - Select **Enabled** to activate the field setting. This allows local administrators to define challenge users and groups.
   - Select **Disabled** to clear the setting.
4. If you select **Enabled**, select **Passcode** or **Password** from the **Logon label** field.
5. Click **Apply** to apply your changes. Then click **OK** to return to the **Authentication** preferences.
6. Repeat the steps in this procedure for the **Send Domain and User Name to Authentication Manager** preference. For example, you may want to enable this preference if you want to send the domain name and the user name to Authentication Manager instead of just the user name. This provides Authentication Manager with more account information to ensure security.

To define the Unlocking Computer setting:

1. Double-click the **Unlocking Computer** folder. You see the **Unlock with RSA SecurID PIN**, **RSA SecurID PIN Time-Out**, and **RSA SecurID PIN Attempts** preferences as shown:



2. Click the preference you want to set. For example, if you want to set the **Unlock with RSA SecurID PIN** preference, click it to open the Unlock with RSA SecurID PIN Properties dialog box:



Note: Click the **Explain** tab to review a definition of the preference setting.

3. In the **Setting** tab, do one of the following:
   - Leave the default of **Not Configured** to leave the setting inactive.
   - Select **Enabled** to activate the field setting. This allows local administrators to define challenge users and groups.
   - Select **Disabled** to clear the setting.
4. Click **Apply** to apply your changes. Then click **OK** to return to the **Authentication** preferences.
5. Repeat the steps in this procedure for each preference you want to set. For example, if you enabled the **Unlock with RSA SecurID PIN** preference, you may want to set the **RSA SecurID PIN Time-Out** and **RSA SecurID PIN Attempts** preferences. You can enable **RSA SecurID PIN Time-Out** to define the time allowed to enter a PIN to unlock the computer in the **Time-out** field. (The preference uses a default of 75 minutes. You can enter a time between 1 to 480 minutes.) Once the time elapses, the user must enter a PIN and tokencode to unlock the computer.

   If you enable the **RSA SecurID PIN Attempts** preference, you can set the number of attempts you want to allow the user to enter the PIN in the **Attempts** field. The preference uses a default of three (3) attempts. You can enter a value of 3 to 10.

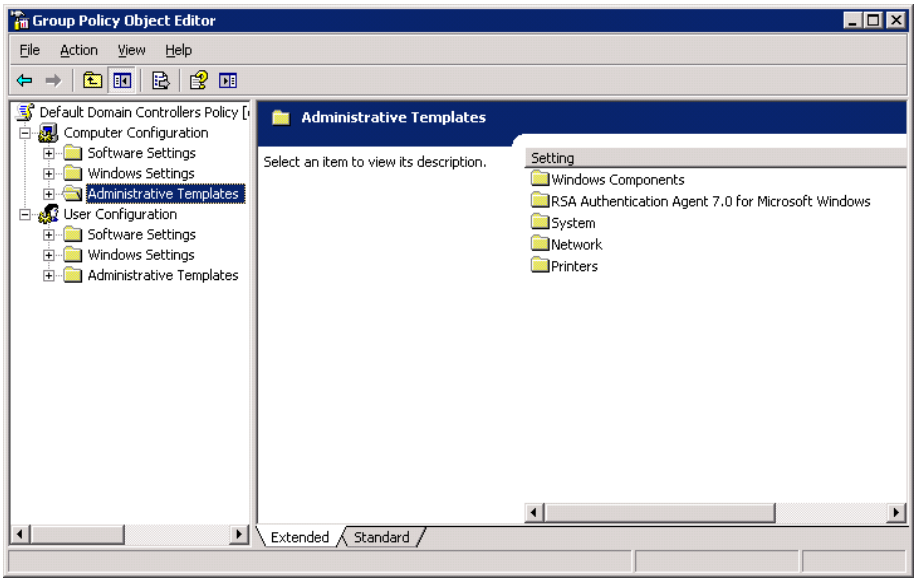
Defining the Password Synchronization Preference Settings

This section describes how to define the preference settings in the Password Synchronization template (**RSA_AuthAgent_PassSynch.adm**).

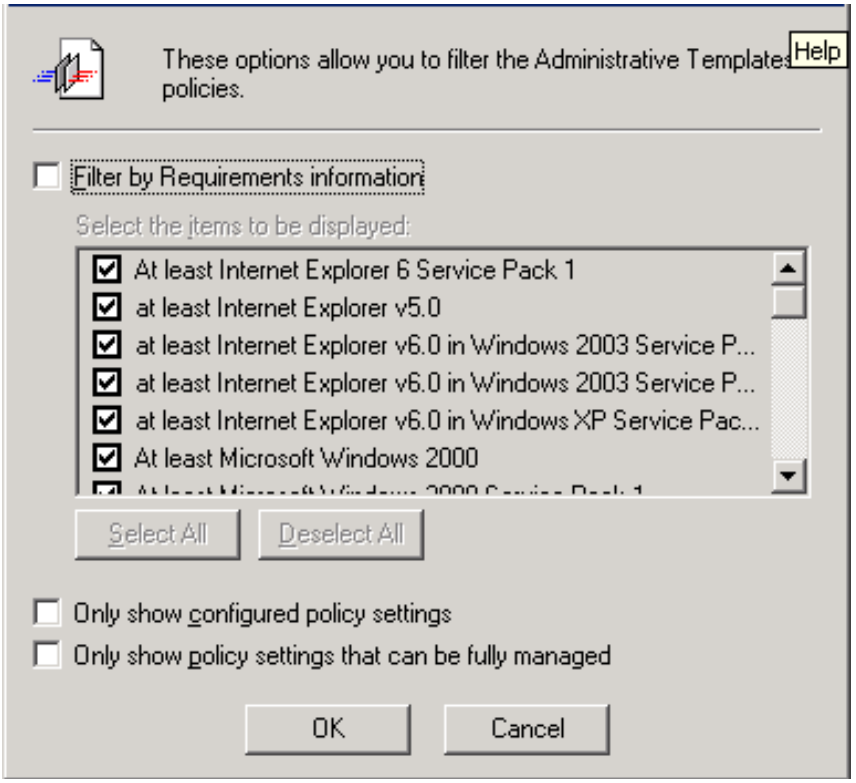
To define the settings in the Password Synchronization template:

1. On the domain controller, click **Start > Administrator Tools > Active Directory > Users and Computers**.
2. In the Active Directory Users and Computers dialog box, right-click **Domain Controllers** under the name of the domain where you want to install the template, and click **Properties**.
3. Click the **Group Policy** tab.
4. In the Group Policy dialog box, click **Default Domain Policy**, and then click **Edit**.

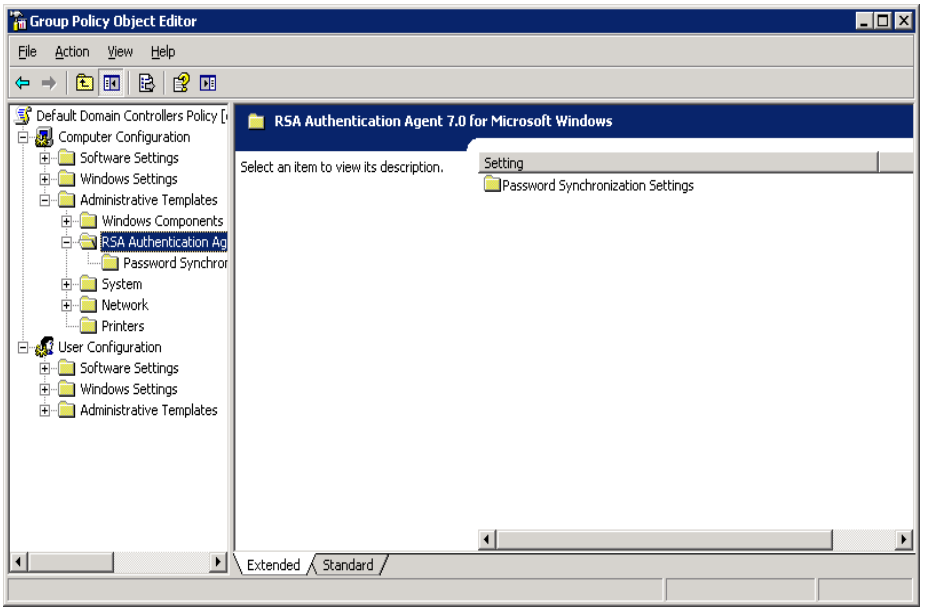
5. In the left pane of the Group Policy window, click **Administrative Templates**. Right-click **Administrative Templates > View > Filtering**.



6. In the Filtering dialog box, clear **Only show policy settings that can be fully managed**. Because the RSA group policies are preferences and not true policies, you must clear this option to view the RSA Group Policy Object templates.



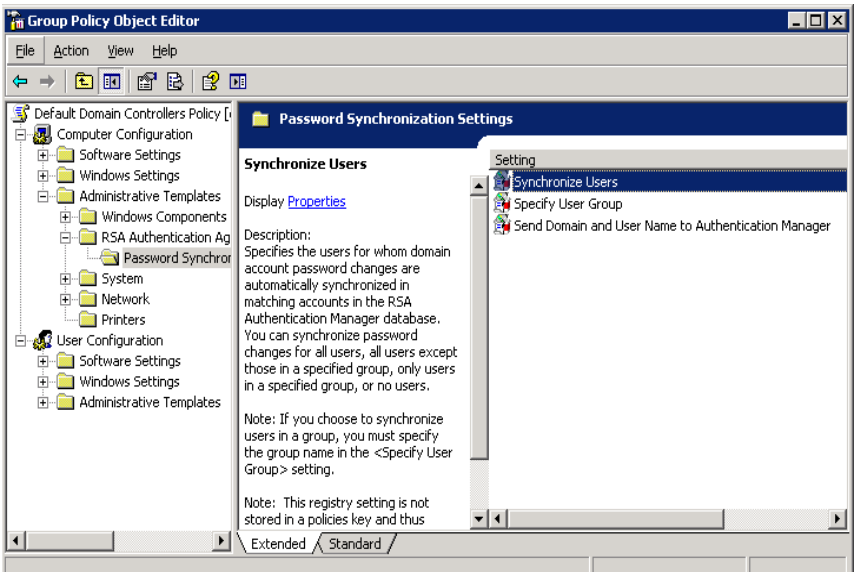
7. Click **OK**.
8. Double-click **Computer Configuration > Administrative Templates > RSA Authentication Agent 7.0 for Microsoft Windows**. You see the Password Synchronization Settings preference folder as shown below:

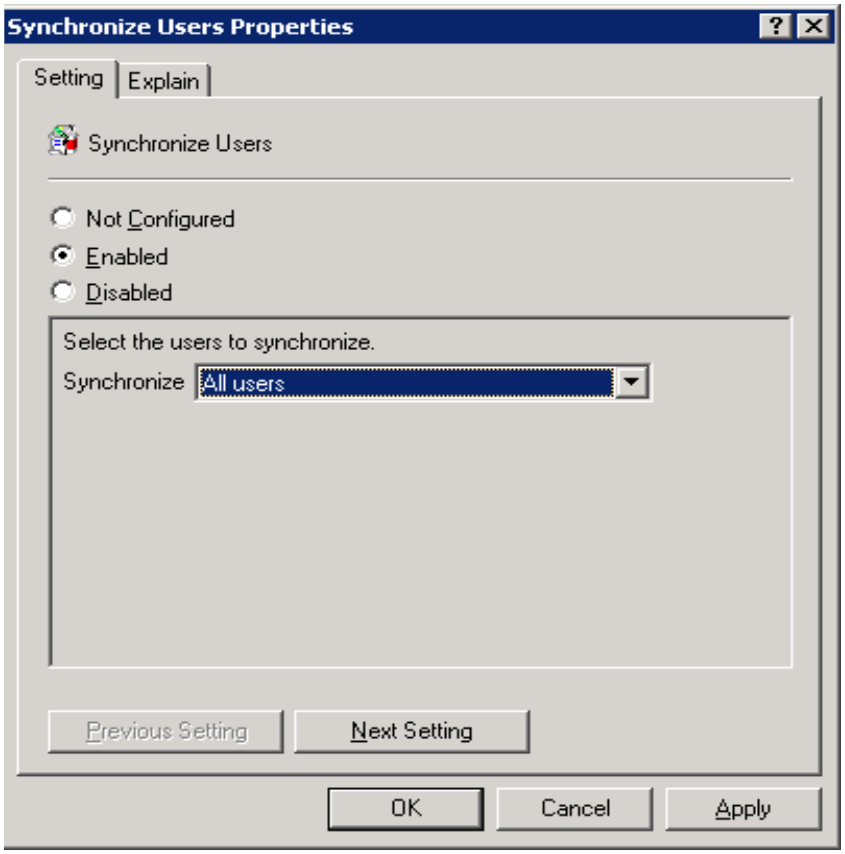


9. Double-click the **Password Synchronization Settings** folder. You see **Synchronize Users**, **Specify User Group**, and **Send Domain and User Name to Authentication Manager** preferences.

To edit the Synchronize Users preference:

1. Double-click the **Synchronize Users** setting to bring up its Properties dialog:



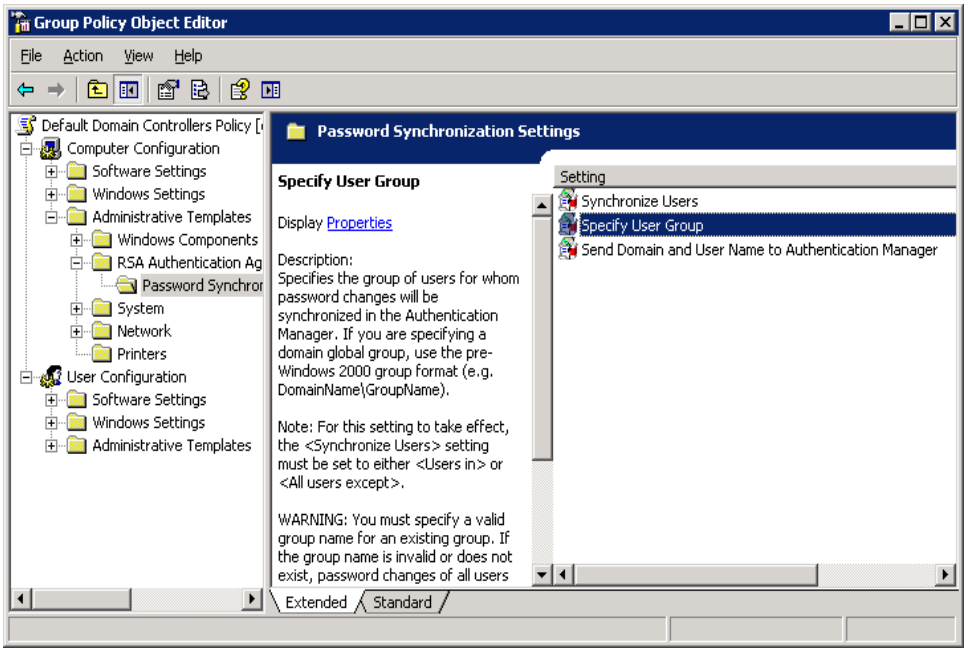


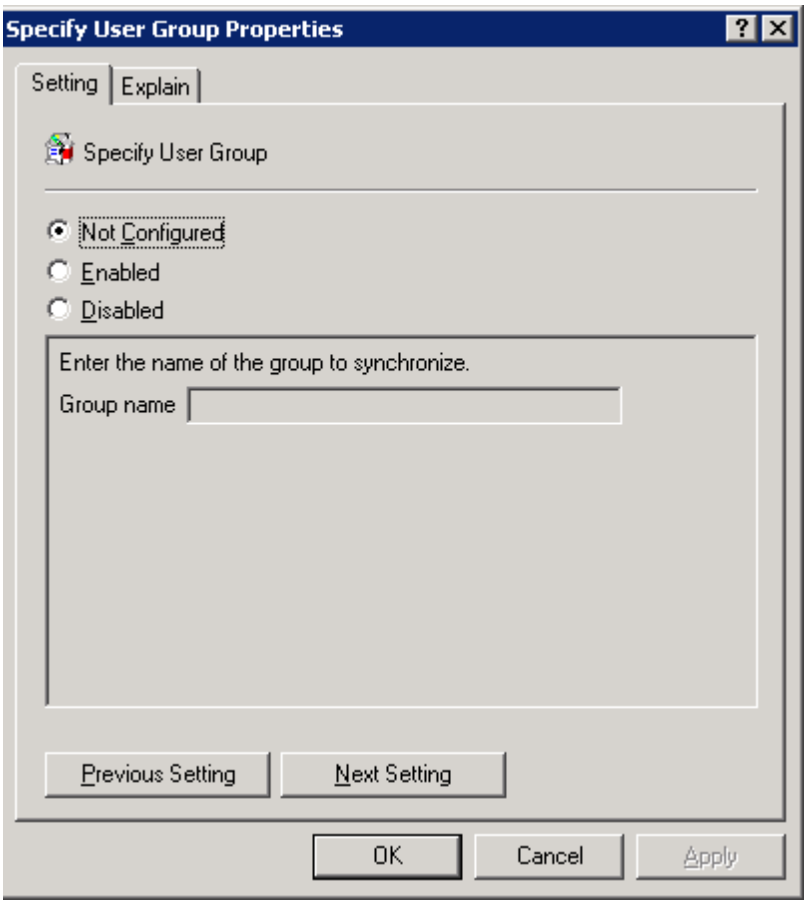
Note: Click the Explain tab to review a definition of the preference setting.

2. In the Setting tab, do one of the following:
   - Leave the default of **Not Configured** selected to leave the setting inactive.
   - Select **Enabled** to activate the field setting. This allows you to specify which users' passwords to synchronize. In the Synchronize drop-down, you can choose **Off**, **Users in *group***, **All users**, **All users except *group***.
   - Select **Disabled** to clear the setting.
3. Click **Apply** to apply your changes. Then click **OK** to return to the **Synchronize Users** preference.

To edit the Specify User Group preference:

1. Double-click the **Specify User Group** setting to bring up it's Properties dialog.
2. To edit the **Specify User Group** preference, double-click the **Specify User Group** setting to bring up it's Properties dialog.





Note: Click the Explain tab to review a definition of the preference setting.

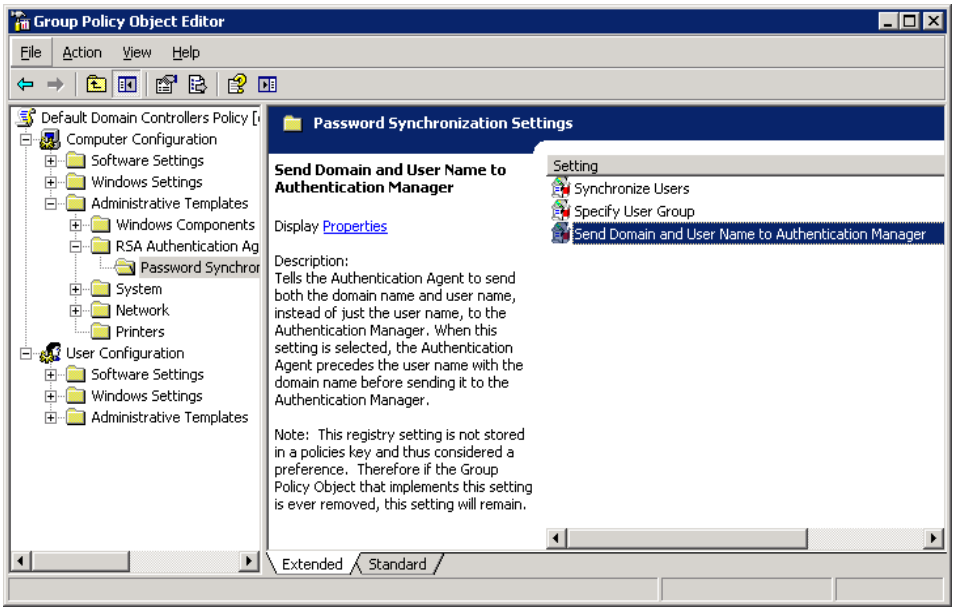
3. In the **Setting** tab, do one of the following:
   - Leave the default of **Not Configured** selected to leave the setting inactive.
   - Select **Enabled** to activate the field setting. This allows you to specify whether the group defining users should be included or excluded for password synchronization.

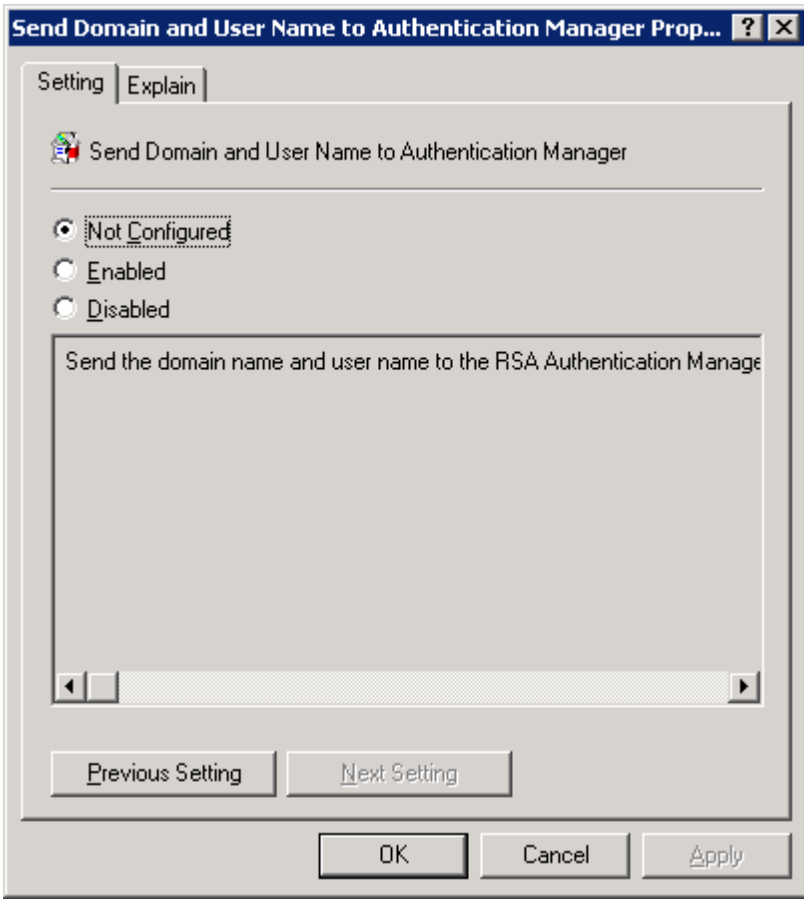
Note: For this setting to take effect, you must set the **Synchronize Users** preference to either Users in *group* or All users except those in *group*.

   - Select **Disabled** to clear the setting.
4. Click **Apply** to apply your changes. Then click **OK** to return to the **Specify User Group** preference.

To edit the Send Domain and User Name to Authentication Manager preference:

1. Double-click the **Send Domain and User Name to Authentication Manager** setting to bring up it's Properties dialog.





Note: Click the Explain tab to review a definition of the preference setting.

2. In the **Setting** tab, do one of the following:
   - Leave the default of **Not Configured** selected to leave the setting inactive.
   - Select **Enabled** to activate the field setting for sending the domain and user name information to the Authentication Manager for defining Password Synchronization.
   - Select **Disabled** to clear the setting.
3. Click **Apply** to apply your changes. Then click **OK** to return to the **Send Domain and User Name to Authentication Manager** preference.

Configuring Preference Settings Using Logon Scripts

As an alternative to using the RSA Group Policy Object template, you can apply preference settings by incorporating them in logon scripts.

The following charts provide details on the location of the root key and the registry settings associated with each Local Authentication preference template.

Credential Provider Filtering Type Setting

The following charts list the key, value name, value type, and options for the Credential Provider filtering type preference setting. They also include descriptions of the key and options.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\Credential Providers
Value Name	FilterType
Value Type	REG_DWORD
Description	Hides or shows the Credential Providers users can access to log on to computers.

Option	Value	Description
Hide Microsoft Password Provider	0	Prevents users from logging on with Microsoft Windows passwords using the Microsoft Password Credential Provider. (Other Credential Providers remain available.) This is the default credential provider filter setting.
Only show RSA Authentication Agent Provider	1	Prevents users from logging on using any method other than RSA SecurID passcodes.
Hide RSA Authentication Agent Provider	2	Prevents users from logging on with RSA SecurID passcodes (PINs and tokencodes). (Other Credential Providers remain available.)
Show all available Credential Providers	3	Allows users to log on using all available Credential Providers. Selecting this option ensures that users can log on to their workstations in case RSA SecurID is not available. For example, you may want to select this option until RSA SecurID is fully deployed throughout your company.

Challenge Setting

The following charts list the keys, value names, value types, and options for the Challenge preference setting. They also include descriptions of the keys and options.

Note: You create challenge groups using the Windows interface. For details on creating Windows groups, see your Windows documentation. If you do not want to create new groups through the Microsoft Windows options, use the default Windows groups. If you create challenge groups for users' domain accounts, local authentication protects access to your company's domain in addition to protecting access to the local computers. You can create challenge groups locally, or you can create them on the domain server. After you create the groups, you specify how Authentication Agent addresses the groups during authentication.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Security Center
Value Name	DisableChallenge
Value Type	REG_DWORD
Description	Prevents local administrators from accessing the **Deny Access to Local Authentication Challenge Settings for Local Administrators** option to determine who Authentication Agent challenges for a SecurID passcode on the local computer.

Option	Value	Description
Disabled	0	Allows local administrators access to the **Deny Access to Local Authentication Challenge Settings for Local Administrators** option.
Enabled	1	Prevents local administrators from accessing the **Deny Access to Local Authentication Challenge Settings for Local Administrators** option.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	Enabled
Value Type	REG_DWORD
Description	Activates the challenge group setting for you to define who Authentication Agent challenges for a SecurID passcode (PIN and tokencode) before allowing access to the computer.

Option	Value	Description
None	0	Prevents Authentication Agent from challenging any users.
Users in	1	Allows Authentication Agent to challenge users in a group for a passcode. **Note:** You also need to set the ChallengeGroup value to the name of the challenge group. See the following charts for details.
All users	2	Allows Authentication Agent to challenge all users, including administrators, for a passcode.
All users except	3	Allows Authentication Agent to challenge all users for a passcode except for those in a particular group. **Note:** You also need to set the ChallengeGroup value to the name of the group exception. See the following charts for details.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	ChallengeGroup
Value Type	REG_SZ
Description	Allows you to specify the group that Authentication Agent challenges for a SecurID passcode (PIN and tokencode) before allowing access to the computer.

Option	Value	Description
Users in	\\ComputerName\ GroupName	Allows Authentication Agent to challenge users in a particular group for a passcode. **Note:** You need to enable the setting to define the users in a group for a SecurID passcode. See the previous charts for details.
All users except	\\ComputerName\ GroupName	Allows Authentication Agent to challenge all users, including administrators, for a passcode except for those in a particular group.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	SendDomainName
Value Type	REG_SZ
Description	Allows the Agent to send the domain and user name to RSA Authentication Manager after authenticating with a SecurID passcode.

Option	Value	Description
Disabled	0	Prevents Authentication Agent from sending the domain and user name to RSA Authentication Manager.
Enabled	1	Allows Authentication Agent to send the domain and user name to RSA Authentication Manager.

Cached Challenge Setting

The following charts list the keys, value names, and value types for the Cached Challenge preference setting. They also include descriptions of the keys and values.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Local\OASVC
Value Name	FailOpenPolicy
Value Type	REG_DWORD
Description	Allows Authentication Agent to use the locally cached policy setting to determine if it should challenge the user for SecurID passcode or not. When you enable the retrieval of challenge settings from the local cache, you must specify how you want the Agent to respond when a cached setting does not exist.

Option	Value	Description
Disabled	0	Prevents Authentication Agent from retrieving the challenge setting from the local cache.
Enabled	1	Allows Authentication Agent to retrieve the challenge setting from the local cache.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Local\OASVC
Value Name	UnknownUsersChallengePolicy
Value Type	REG_DWORD
Description	Allows Authentication Agent to challenge the user for a SecurID passcode if the cached settings do not exist.

Option	Value	Description
Do not challenge	0	Prevents Authentication Agent from challenging the user for a SecurID passcode. **Note:** If set to 0, you must set FailOpenPolicy to 1.
Challenge	1	Allows Authentication Agent to challenge the user for a SecurID passcode.

Windows Logon Setting

The following charts list the keys, value names, and value types for the Windows Logon preference setting. They also include descriptions of the keys and values.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	LogonPromptPassword
Value Type	REG_DWORD
Description	Sets the logon label for the Authentication Agent Credential Provider to **Password** or **Passcode**. Users see the field label you set when they attempt to log on to the computer.

Option	Value	Description
Passcode	0	Shows a logon field label of **Passcode**.
Password	1	Shows a logon field label of **Password**.

SecurID PIN Setting

The following charts list the keys, value names, and value types for the SecurID PIN setting. They also include descriptions of the keys and values.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	EnablePinUnlock
Value Type	REG_DWORD
Description	Allows the user to unlock the computer by entering a SecurID PIN within a set amount of time after locking the computer. Once that time expires, users must enter a passcode to unlock the computer. For example, if you do not set this option, users must always enter full passcode (PIN and tokencode) instead of just a PIN to unlock the computer.

Option	Value	Description
Disabled	0	Requires the user to enter a passcode to unlock the computer.
Enabled	1	Allows the user to unlock the computer with a PIN within a set amount of time.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	PinLifetime
Value Type	REG_DWORD
Description	Number of minutes a user has to unlock the computer with a PIN before the Agent requires a full passcode.

Option	Value	Description
Time-out	1 to 480 minutes (default = 75 minutes)	Number of minutes between 1 to 480 before the Agent requires a passcode instead of a PIN to unlock the computer.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDGINA
Value Name	PinAttempts
Value Type	REG_DWORD
Description	Number of times a user can enter an invalid PIN before the Agent requires a full passcode.

Password Synchronization Setting

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDNETWORK
Value Name	Enabled
Value Type	REG_DWORD
Description	Activates/deactivates the domain user password Synchronization setting:

Option	Value	Description
OFF	0	Deactivates password synchronization
In *group*	1	Sets password synchronization for users in a group
ALL	2	Sets password synchronization for all users
Except *group*	3	Sets password synchronization for all users except the users in a group

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDNETWORK
Value Name	ChallengeGroup
Value Type	REG_SZ
Description	Allows you to specify the group to govern the inclusion or exclusion of domain users for whom to synchronize passwords.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\RSA\RSA Authentication Agent\CurrentVersion\Settings\SDNETWORK
Value Name	SendDomainName
Value Type	REG_DWORD
Description	Allows the Agent to send the domain of the domain users whose passwords will be synchronized.

Option	**Value**	**Description**
Disabled	0	Prevents Authentication Agent from sending the domain of domain users to the RSA Authentication Manager
Enabled	1	Allows Authentiation Agent to send the domain of domain users to the RSA Authentication Manager